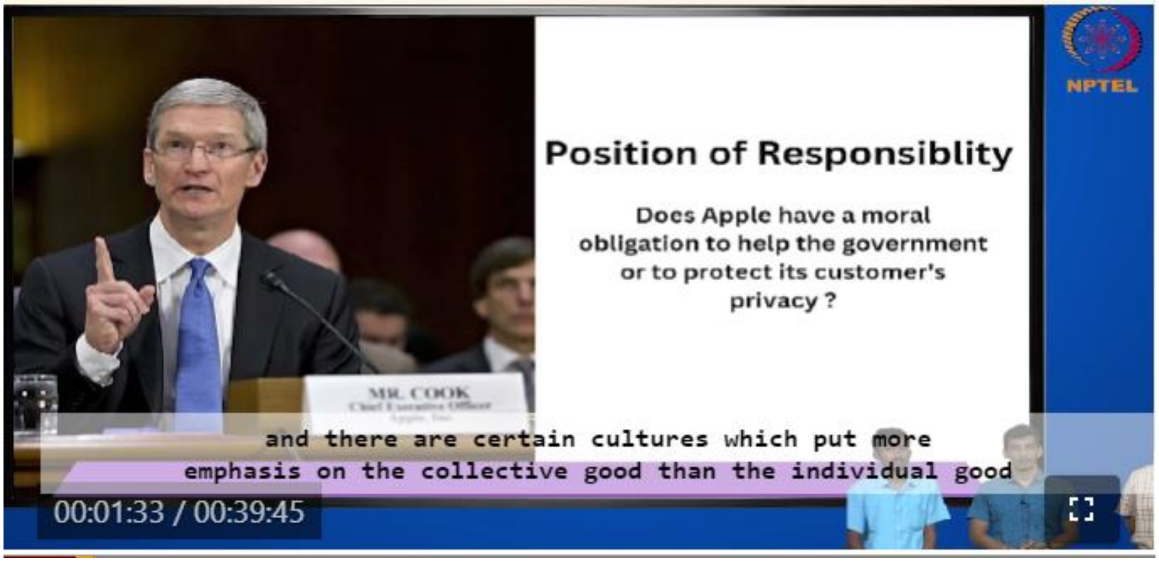
Course Name: Cyber Security and Privacy
Professor Name: Prof Saji K Mathew
Department Name: Department of Management Studies
Institute Name: Indian Institute Of Technology Madras, Chennai
Week: 14
Lecture: 42

So it created a very big position of responsibility for Apple whether and the citizens of US were divided in their opinion. Many people who were concerned of their privacy said that, supported Apple in its stance that they should never compromise the user's data and privacy with the government. But there were also many people that, they wanted Apple to comply with the government for their own safety. Their point was that Apple should, they wanted their safety or their family's safety more than the privacy. So this raises a question, like does Apple have a moral, not only Apple does any organization have a moral obligation to help the government or to protect its customer privacy. So what will be your opinion, like any organization or with the devices you use will you be comfortable, like sharing the data with your government for the safety or will you value privacy more than safety? So for this point it is, there is a lot of the cultural aspect which comes into play and there are certain cultures which put more emphasis on the collective good than the individual good and that tend to be more okay with sharing data versus an individualistic society which tends to, which focuses on prioritizing personal data privacy even if it comes at a certain cost.



Position of Responsiblity

Does Apple have a moral obligation to help the government or to protect its customer's privacy ?

and there are certain cultures which put more
emphasis on the collective good than the individual good

00:01:33 / 00:39:45

So that is why we are seeing that in, for an organization like Apple which functions in different countries, that taking an extreme position and holding on to it becomes tough especially when it is using it as a strategic motive that it wants to highlight the company as somewhat, a company which holds privacy as a top priority irrespective of the countries but when it goes to China, there are certain things which the company gives away on the same aspect. So it is basically looking at it from, Apple is looking at it from a business perspective and it is trying to differentiate itself but at the same time in China when it sees that profits can get take a hit, it modifies its strategy a little bit. So whether a company has a moral obligation to help the government, it is you consider a lot driven by the law of the land itself and the law would be driven, is influenced by the culture, right. So, so that is where an absolute answer to this question may be tough.

Yes, you are correct even my batchmate also explained how different, using the previous survey how different countries have different view about privacy of data. So that is a point to be noted, how culture, if culture has a influence on this, such questions. There has to be a trade-off between privacy and security. For example, government continuously snooping on all the people whether they have any links to terrorists or you know continuous snooping just mere to, mere for data collection would not be the way forward. Instead if there is any terrorist link or in the previous case video that you showed, there Apple should have a way to share the information.

For that the three key methods that you showed, like they are having shared keys, Apple and government, that could be a way forward and for that Apple will have to bear the cost. I would feel that first of all, Apple has a moral obligation to its customer and it has to protect the customer's safety and one part of safety is privacy, other part of safety is bodily harm. So, since Apple cannot protect a person from harm, it needs to help the government which in turn will protect the person from harm. So tomorrow if a bomb goes off in an Apple store by a terrorist, who used an Apple phone, so it has lost more customers in order to save one customer. So keeping this in mind, Apple should perhaps help the government in doing what it cannot, it is out of scope for Apple to do.

So, that is my. Yes. So in this, is the same point which I saw in many forums, like online debates that helping the government is a, indirectly you are helping your customers, that is one point. I think what Apple says here is that we manufacture a locker and the locker has keys and we sell the locker with the keys to the customer. Now the keys is, key is with the customer, we do not hold the key because the locker belongs to the customer.

So if the government comes and ask Apple for what is stored in the locker, Apple says, no, we do not have the keys. We already sold it to the customer. So ask the user, that is the position, but the, I think the weakness of that argument is in instances where a person dies and the password as a key is not existent in which case, there should be a way to enter the locker, open the locker. That is I think, that is a, in my opinion, that is a fair argument for national safety, security. Otherwise how do you actually catch criminals and bring them to, you know ensure justice to the country? So that is one aspect, but the other is to say that, well you have a house or you have a locker and there should be a separate key which is created for government and the government should always be keeping that key and it can come and open your locker anytime.

And that is the permanent back door which actually governments want, anytime access to locker or phones owned by citizens. I think these two aspects are mixed in the case as you go, the what kind of access is what government is looking for, FBI is looking for, is it case to case or is it continuous? So it is about creating a back door permanently. So, which is a matter of concern. So moving to a similar case, here in the previous case we saw how it was all about national security, but there is a recent case. It is about tracking the data for safety of the, to counter such a major pandemic.

So you all must have used Aarogya Setu. It was a, it was a encouraged by Government of India to track the users for the health adversary, but there was a similar app developed by Google and Apple together. It was same. It was a used for contact tracing. So let us look at some technical details how it was.

Okay. Battling COVID-19 is an unprecedented global challenge. To get communities around the world back up and running as quickly and safely as possible, public health authorities are building smart phone apps to help with contact tracing. Contact tracing is one of the best ways to stop a virus from spreading. It can take thousands of disease investigators to alert everyone who's been in contact with people who've tested positive. But even if disease investigators do their jobs perfectly, alerting the people a COVID patient does not know or can not remember is incredibly difficult.

Smart phone apps that the public health authorities built can help people at risk of infection get notified much more quickly. But a contact tracing app works best when more people download it. And being asked to download an app without knowing how it will handle your personal information might cause people to worry about their privacy and they may not feel safe participating. That is why engineers at Apple and Google have been working together to make public health technology that protects individual privacy, so that people never have to choose between their privacy and the health and safety of their community. You are probably wondering what that means and how that all works.

And we are going to walk you through it in a second. But first, let us be really clear about a couple things. First, apps using this system cannot track your location. And second, this system does not share your identity with Google, Apple, or other users. Here is how that works.

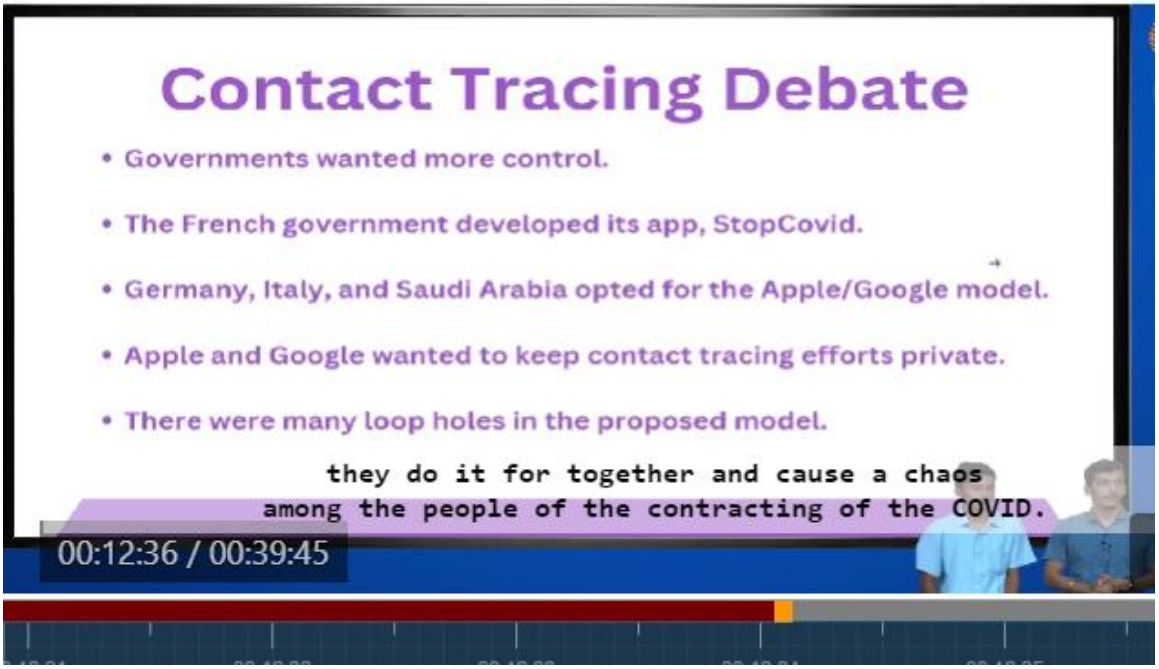
For every phone that is opted in, our technology disguises your identity by generating a random sequence of numbers that change every few minutes. Then using Bluetooth, any time your phone detects another phone close by that is also opted in, the two exchange those random numbers. If in the future someone is positive for COVID-19, they can report that positive result in our app. Any phones that had exchanged random numbers in the last 14 days will receive a notification that they may have been exposed to COVID-19 without revealing their identity. Public health authorities can then help anyone at risk get testing and treatment.

But it is up to all of us to help with contact tracing. Do your part and look through your public health authority app that uses this exposure notification system. The more people who participate, the sooner we can beat COVID-19 and get our communities back on their feet. Okay, so this was the solution proposed by Apple and Google together to counter the COVID-19 and worked as a contact tracing solution. But there were, just like the previous case study, there were many controversies surrounding it with government and with the people.

So first controversy was the government wanted more control as you can, as you have seen in the video that no user data and location was tracked by the both Apple and Google. So government wanted a more controlled app or a more controlled solution, like they can track the user who have been contacted and also their locations. But Apple and Google refused for it. There was a major backlash from the French government and even the health minister quoted that the companies like Apple who have never been in a good situation of economy are not helping the government to counter the crisis. Instead they developed their own app, Stop COVID just like Aarogya Setu in India.

But there are also other countries like Germany, Italy and Saudi Arabia who use this model. So the major issue was with the data collection and tracking. Apple and Google wanted to keep the efforts private that they were not focused on the location and other data. They wanted it to be more private to the user itself. But the government and other health organization were more focused on getting, understanding the locations of the contacted patients.

And also there were many loopholes with the proposed model is that the first one was that in the, in search app the user has to notify to the app that I am, I have been



Contact Tracing Debate

- Governments wanted more control.
- The French government developed its app, StopCovid.
- Germany, Italy, and Saudi Arabia opted for the Apple/Google model.
- Apple and Google wanted to keep contact tracing efforts private.
- There were many loop holes in the proposed model.

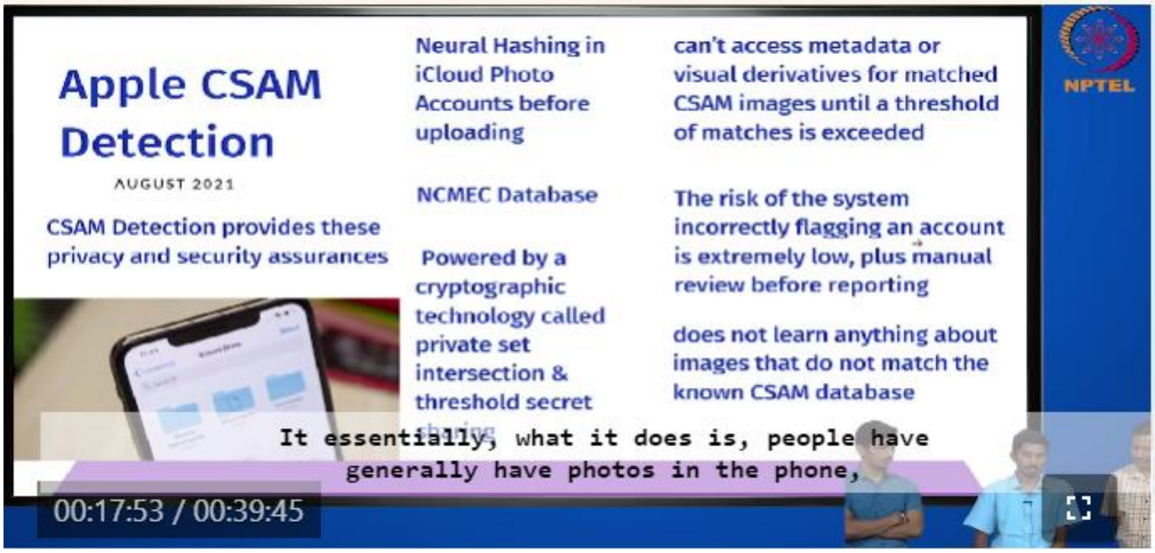
they do it for together and cause a chaos
among the people of the contracting of the COVID.

contracted with the virus. But there were many reports of fake reporting also and which might cause chaos among the people and imagine a group of people, they just to cause chaos in the country, they do it for together and cause a chaos among the people of the contracting of the COVID. So that was a big debate in the contact testing, how data needs to be handled in such situation. So as a result of all these incidents of privacy, also safety there were also one incidents where the companies which are dependent on the organization like Google and Apple, who collect the data, they and the Facebook organization is reliable on the Apple and Google for collecting the data, they face many problem due to change of regulation and policy by Apple. One such incidents was when in iOS 11, in iOS 14 Apple change its policies in iOS 14 the user had access to what an app, a particular app is tracking what kind of data and it also had a option to simply opt out of the tracking which was heavily criticized by the Facebook because it, as you can see it suffered around 10 billions of revenue hit because of this feature and not only, it was not only Facebook but there were around 16 marketing agencies that wrote to the Apple for the displeasure for this feature.

But there was also positive impact. This, such incidents of hailing privacy over other aspects created a trend among other companies too. Similarly Android, Google also gives similar feature in Android OS 11 and it was followed by other organization too, like Zoom also gave into an encryption for their video calling and there were also many organization that emerged which considers security as their main criteria or their main feature, similar there is a similar organization will have a comparison is like a DuckDuckGo which is a privacy focused search engine as opposed to the Google. They promise the user that there would not be any tracking or any data collection from their side which is a, which is what

Google does to give a better user experience and apart from DuckDuckGo there are also many other apps like Signal, Brave browser which are more focused on user privacy. So it gives a, it brings us to a question, like such developments or such incidents have increased valuation of privacy among the user.

So I would like to ask the same question to you, like are you more focused on the privacy rather than services, like are you using such apps like DuckDuckGo, Brave browser or Apple devices just for the privacy? Anyone of you? Are you using any DuckDuckGo, Brave browser or Signal? You are using so. I am using DuckDuckGo, Tor on Android as well as laptops. So is privacy your main concern for using it? Yes, especially transactional this thing but there is a problem with Tor when it comes to commercial or like financial transaction issue because even all apps, even banking apps they need access to your locations and all. So does not work very well but yes to gain information and all, yes that is a, it is a good idea, it works with that. Anyone else? Okay so to shed more light on this question, we will look at a recent survey which said that, like these days around 89% care more about their data privacy and 40% were willing to spend time and money to protect the data and also 29% people switched their apps or services that were, that they were using just because of privacy concern, just like in the recent incident, was that WhatsApp had updated their privacy policy after acquisition by Facebook and like, they were going to use the user data for marketing and many people had, not many, small fraction of people had migrated to Signal messenger for the same reason and there are also 90% of consumers are somewhat too very concerned about the privacy.



Apple CSAM Detection

AUGUST 2021

CSAM Detection provides these privacy and security assurances

Neural Hashing in iCloud Photo Accounts before uploading

NCMEC Database

Powered by a cryptographic technology called private set intersection & threshold secret sharing

can't access metadata or visual derivatives for matched CSAM images until a threshold of matches is exceeded

The risk of the system incorrectly flagging an account is extremely low, plus manual review before reporting

does not learn anything about images that do not match the known CSAM database

It essentially, what it does is, people have generally have photos in the phone,

So it shows that such incident which have happened in past have given a more concern, have increased the concerns of privacy among the users. So I will just hand over to Sanjay. And now we will see a very recent development of Apple in relation to privacy. So as you can see, this is basically called CSAM detection. It is, abbreviation is Child Sexual

Abuse Materials.

It essentially what it does is, people have, generally have photos in the phone, like before uploading the phones to either go, like drives or any cloud storage, like here what Apple wanted to do is to find a middle ground in maintaining privacy as well as protecting the threats. So what it does is essentially it scans for CSAM content in the respective iPhones but without compromising their user's privacy. So what it essentially, how it works is, like it initially generates a neural hash. So what is this, hash is like, it creates a, it is called a neural hashing algorithm what it creates, it creates a hash which is very context specific. It is not similar to the file hashing we do on computers which, even if we change one bit of data, the hash value changes.

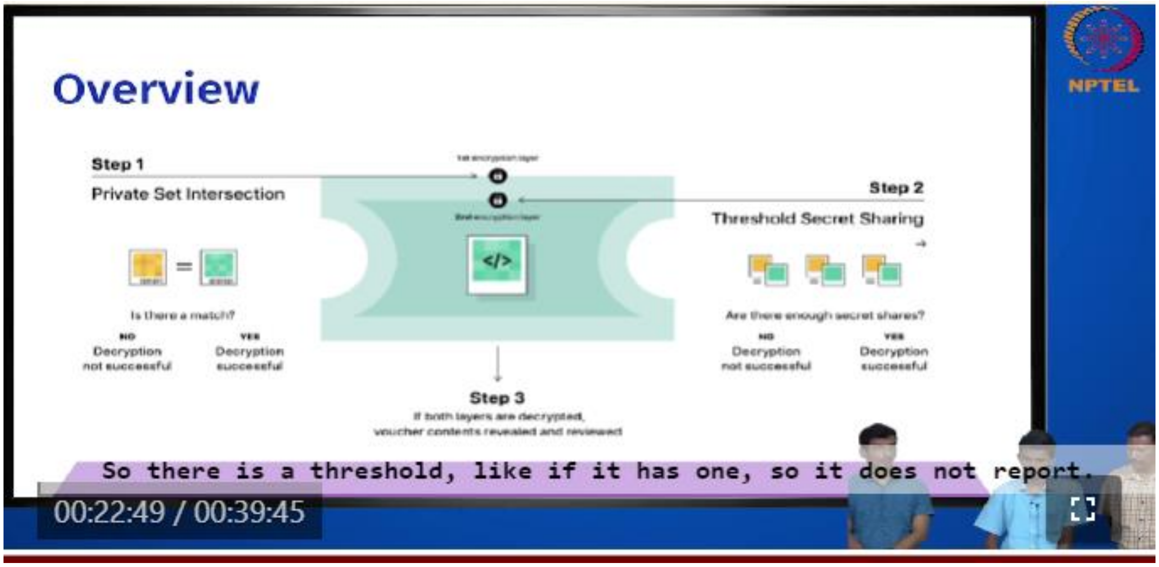
So here it is context specific, what so? So if you see, so if you see these images, the first two images are, so as humans can see it, these images are basically same without the colour. So if you, if you take the very file hashing, so what computer thinks, it, these two are very different files. So in neural hashing what it does is, it creates a hashing but as we can observe it creates the same hash for both these images but if you see, compare it to the last one, it is entirely completely different image. So it creates a different hash for different images but if it is very similar as observed by humans, it creates the same hash. So CSAM detection provides these privacy and security assurances to users.

So before uploading also, we have to note that this neural hashing occurs in device itself, not, it does not happen in the servers of Apple. So what they do is they create the hash in the device. So if the hash values, like the CSAM, they the government or NCMEC, it is the National Center for Missing and Exploited Children database. Also there are other independent data services which provide these CSAM contents from various location, like dark web, like they provide the database. So when a photo is being uploaded to the iCloud it, like it compares the hashes to the hashes of the existing database.

So it is powered by two technologies, the one is called private set intersection. So what it does is, it essentially matches it is, essentially checks whether the images are matching with the database. So here Apple what to prevent the, to protect the privacy, it prevent, it created such created a technology such that it is encrypted double. So it protects the privacy of the people. So it also assured that the meta data is, you know if it, you know in case it detects one like CSAM content, it is does not immediately report to the law enforcement.

So it has a certain threshold before it is being reported. Now also, even if it finds after the threshold, it is manually reviewed before reporting it to the law enforcement officials. Also for, like there would be multiple photos of random contents, so it does not, like if it does not find any CSAM content it is, like the Apple would not learn anything from it, like also does not report the entire usage, entire data to the Apple or either governments. So this is how it works. So first it essentially creates a image hash, then it, like it, the it, like it is as I mentioned it is in the device, so it creates a safety voucher.

So then it uploads these pictures to iCloud. So as I mentioned before, so the private intersection, private set intersection what it does, it essentially compares if there is a match. So if there is a match, so it will decrypt. So also I said, like Apple does not you know violate the privacy of the person. So there is a second encryption which is done by technology called threshold secret sharing.



Overview

Step 1

Private Set Intersection

Is there a match?

NO
Decryption not successful

YES
Decryption successful

1st encryption layer

2nd encryption layer

Step 2

Threshold Secret Sharing

Are there enough secret shares?

NO
Decryption not successful

YES
Decryption successful

Step 3

If both layers are decrypted, voucher contents revealed and reviewed

So there is a threshold, like if it has one, so it does not report.

So there is a threshold, like if it has one, so it does not report. It has a certain threshold, like it has to flag this, like certain number of CSAM content to flag this, flag the alarm. So only if both of these matches, so both layers are decrypted and then only there is images being revealed and then also it, then also after the collection of data, it is the manual process of reviewing is undergone before reporting it to the law enforcement officials. So there are multiple checks and steps to prevent, to protect the privacy of individuals. But as we can see in this news clipping, it is the, this is the case of Google using a similar kind of technology, like but in this case as we can see it, it falsely triggered an alarm for genuine case.

So father took his picture of his younger toddler son. So what it does, it detected as a CSAM content and it reported to the law enforcement directly, without any checks or manual review process. So it caused major embarrassment on the consequences for him but finally, but the police did not file any charges due to its legitimate case. But it caused, it also caused him huge embarrassment and cost in a society. So also what Google did is, they did not, they locked the account and did not restore it back.

So the entire history and collection of photos and all were destroyed. Okay just to, sorry to interrupt you here, to bring the discussion back to the case because we need to be within the scope of the case. So there may be recent developments which are related, before as the time is ending, so I just want to give couple of observations. One is in the case A which you discussed, there is a specific culmination of this case which is the San Bernardino incident where militants actually killed 14 people and the FBI was doing the investigation and that is the point when Apple refused to create a back door for FBI and that actually blew, that incident blew up because government and government agencies believed that Apple is not cooperating with an investigation which is having national safety implications and FBI also blamed that encryption is being used as a marketing pitch by Apple. So there are several indications in the case that it is not genuinely in the interest of people's privacy that, Apple is taking that position but it is for the marketing purpose.

To position their product as highly privacy preserving and in order to protect that position or in order to strengthen that position they were taking a stance. Although if you take a larger view anyone would say that in that particular case, you know a company should cooperate with the investigation. Only for that case. It is not that you create a permanent back door but the case was very serious. Do you know what happened further because the FBI, government has to do investigation they have to actually, they will go out anywhere to get information and track down the criminals.

If you read what actually happened in that case. They cracked it. FBI cracked it. They went to Israel and they were able to crack it. Although Apple did not disclose. What do you think about that condition? How it would have affected Apple? Plus see, whatever Apple claimed that their products are very secure and you know nobody can actually access, Israeli hackers actually proved it wrong.

If they want, they can actually crack even Apple.. So, yeah, so there is a lot of evidence that Apple is actually doing. So that also made the vulnerability of Apple devices open. So it became rather an embarrassment for the company claiming that nobody can, not even the government can but actually a hacker can. So I think that ending of the incident was not very much in the favour of Apple and therefore this particular hard stance of privacy versus safety, when it comes to extreme cases like this, perhaps was not justified.

This is what I think. That is one take away from the first case and we also clearly see there is, it is a marketing pitch. Apple versus, Apple which, whose revenues, as you rightly showed comes from selling high end products, not from databases or online advertising.

So there are other companies like Google and Facebook, whose revenues actually majorly come from online advertising. And advertising industry requires data. So that is a business model and if it is privacy completely protect, no access to personal data then that industry cannot exist.

So that is a hard reality. So it is also sales pitch or marketing pitch that is going on in all these cases which is quite visible. And the second case that you discussed as you are wrapping it up, of course, you are going to other developments. But again the case writers are bringing a situation where it was about health of people. Pandemic, it was a pandemic condition and so there were solutions developed by individual governments for contact tracing.

For example, Indian government developed Aarogya Setu. But Aarogya Setu you must have read, it was not very successful. And immediately the opposition actually brought out the government is doing surveillance and the government is collecting this data but it may be solved, it may be abused and so on. So that is what opposition will do. But somewhere if you check the government stance also, there was actually a workshop on this in IIM, Bangalore on Aarogya Setu's transparency. Government finally said well, Aarogya Setu is built on open source platform.

So the user end is open, the code is open. But the server side code was not open. So once the data goes to the server that part of the whole software that they built was not made on open source. So that again brought some sort of lack of clarity or transparency for users to share data. So in these cases the real debate is between governments outright back door access to all devices for the purpose of governance and citizens concerns that their private data can be abused by government.

That is an issue which is difficult to resolve. Continuous monitoring versus case to case investigation and back door entry as a permanent need for governments. So that is an ongoing debate and we have to watch and wait what is going to happen in this sphere. And there are companies which thrive on privacy as a business strategy and they would like these cases to be highlighted in public or in media and that actually of course, brings lot of publicity or marketing or it is in the favour of those companies like Apple. Okay, latest what do you think that particular incident, you know Apple changed its policy in 2017. I guess, you know they actually gave an option to the iPhone user called ATT, App Tracking Transparency.

I think app tracking transparency, in the sense other apps in your iPhone can track, one app in your iPhone can track your activity with the other apps, perhaps what pages you browse etc. So that access of apps to other apps is a feature that the user can decide now in iPhone. You can switch it off which actually affects the advertising potential of companies. And that is what you showed, the advertising revenues of Facebook and Google substantially got affected. But what is Apple trying to do through this? They want to bring more transparency to the user, what is happening on their phone.

Okay, so it seems to be advocating privacy and used to be protecting the privacy concerns of individuals but it is hugely affecting the other businesses revenues. But is there a competition between Apple and Google? Because Google is basically, its most revenues comes from advertising.

Advertising. That is their revenue. Apple sells products. So they are not competitors per se. So how should, why should Apple create a feature that will kill a company which is not a direct competitor? Which is not a direct competitor, because one is selling, one's business model is based on advertising, other's is based on selling products.

That is operating system, that is open. Okay. Okay. So how do you? So it is iOS versus Android. Okay. What about Facebook? There is no competition on operating system. That is my question. Why Apple should actually hurt, why should Apple hurt Facebook's revenues? Yeah, they showed 10 billion loss of revenues after Apple changed its policy.

The ATT, user can divide, decide. But there have been reports that, no, that is possible. We could be the millennials now, Sir. As iPhone user, one may be using apps from Facebook or Google Chrome etc. So in that sense if Google or Facebook has more bargaining power than Apple, then it becomes a disadvantageous position for the company. So it would try to increase its own bargaining power by trying to limit Facebook or this.

What is the Apple versus Facebook experience? For that ATT policy, it is not about only the ATT policy, even though the iPhone is created in an operating system level and secure, the apps which is created by the other users and it has been downloaded by the user who is willing to download and use it, the apps may be malicious also. So the ATT policy is created, so that there are some, even in India, the government has banned some more apps which is not to be used in Android. So the people may be aware of that, whether the app is tracking it or not. So Apple gave a chance to know that if you are not willing to use an app, you can make sure what it has been tracking or not. There were a lot of cases where the Apple users were using apps and were testing it for their platform and their Android apps are not protected.

So the app which iOS has specifically developed for their platform, who will be able to work on this ATT? Where are they collecting it and now if you do it, they will not collect it. Do we have some information to that? What is the ratio of Android users to Apple users? Which will be, you know, Android and Apple users being in the platform. Yeah, I think they may not have data because this is instantly coming but the point is, Apple is also into advertising. So it is trying to kill its advertising competitors.

Because with ATT, Apple advertises differently. So the digital advertising market has grown. If you look at the advertising trend, you know, so in recent times the online advertisements or the digital advertisements exceeded the traditional advertisements. So therefore the advertising industry is moving largely towards digital advertising and Apple wants to have its share there. So when it introduced ATT, Apple is actually encouraging advertisements through apps, not through search engine or Facebook platforms, through apps, Apple apps which is in the iPhone. So basically by hurting Facebook and Google, it is actually trying to increase its share of advertising revenues.

So you see how smartly these policies can be communicated. One is we are trying to protect your privacy. The other is we are actually trying to increase our advertising revenues. So this is actually the smart positioning this tech giants do. So for users it sounds like, you know, they are our Gods.

They are so much interested in our welfare. But these are carefully crafted business strategies. Recently we have to pay, use only through Apple Pay. Earlier it was card and other payment option was there.

Now it has been disconnected, only through Apple Pay. People may think it is privacy. But for every transaction, the other banks has to pay a commission to make a transaction.